SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET

A STAFF REPORT

PREPARED FOR THE USE OF THE

COMMITTEE ON ENERGY AND COMMERCE

U.S. HOUSE OF REPRESENTATIVES
109TH CONGRESS

JANUARY 2007

SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET

BIPARTISAN STAFF REPORT FOR THE USE OF THE
COMMITTEE ON ENERGY AND COMMERCE

January 2007

I. Key Findings

The Subcommittee on Oversight and Investigations examined several different components of the U.S. effort to combat the sexual exploitation of children over the Internet. Broadly, these entities included: (1) U.S. law enforcement; (2) the National Center for Missing and Exploited Children ("NCMEC"); (3) Internet Service Providers ("ISPs"); (4) the financial services industry; and (5) social networking websites. The Subcommittee also reviewed the efforts of several foreign governments and industries with respect to the sexual exploitation of children over the Internet, including the United Kingdom's Home Office, the Internet Watch Foundation ("IWF"), the Child Exploitation and Online Protection ("CEOP") Centre, Interpol, the European Union, the Dutch National Police Agency and Ministry of Justice, and Europol. The Subcommittee's investigation also encompassed examining Internet safety educational programs, as well as exploring issues related to the psychology of pedophiles and online child predators in order to educate parents and children on how children can avoid becoming a victim. Key findings from the Subcommittee's investigation include:

- Crimes involving the sexual exploitation of children over the Internet are a growing problem in the U.S. and around the world, due to the ease with which pedophiles and child predators can trade, sell, view, and download images of child pornography from the Internet.

- The number of sexually exploitative images of children over the Internet is increasing, the victims are becoming younger, and the substance of the images is growing more violent.

- Commercial websites involving the sexual exploitation of children over the Internet are a growing and lucrative business. Current estimates indicate that on any given day there may be more than 100,000 sites with commercially available child pornography and that this is likely to be a multi-billion dollar-a-year industry.

- Together with the development of digital photography and web cameras ("web cams"), the ability to communicate anonymously over the Internet through online chatrooms, Instant Messaging services, and social networking websites has made it easier for pedophiles and child predators to contact children and to "groom," or befriend and seduce, them. The Federal Bureau of Investigation ("FBI")

estimates that 50,000 child predators are online at any time searching for potential victims.

- The U.S. law enforcement effort to combat online child pornography involves several different federal agencies, with sometimes overlapping jurisdiction in these cases, as well as federally funded state law enforcement officers specially trained in these cases, referred to as Internet Crimes Against Children ("ICAC") Task Forces. Each of these agencies performs vital investigative functions necessary to combat the sexual exploitation of children over the Internet. Federal law enforcement agencies either need increased funding or better prioritization and organization within their agencies, or both, specifically to combat child exploitation over the Internet, including additional agents dedicated to investigating these types of crimes, additional forensic laboratories and specialized training for investigating these cases.

- The U.S. Postal Inspection Service ("USPIS"), which has a long-standing role in investigating cases involving the sexual exploitation of children, does not currently have statutory authority to issue administrative subpoenas in child exploitation cases, whereas other federal agencies, such as the FBI and Immigration and Customs Enforcement ("ICE"), now part of the Department of Homeland Security, do have this power. In order to further enhance the ability of the USPIS to investigate child sexual exploitation crimes, an amendment to 18 U.S.C. § 3486 should be considered by Congress to include authority for the Postmaster General to issue administrative subpoenas in criminal investigations involving child exploitation.

- While the federal sentencing guidelines for criminal offenses relating to the sexual exploitation of children involve strict penalties, there is a wide discrepancy in state criminal codes both in covering all the substantive offenses, as well as, in sentencing. Because approximately 70 percent of all cases involving the sexual exploitation of children over the Internet are prosecuted at the state level, state legislatures should consider enhancing the penalties for these offenses and, in some instances, passing additional criminal laws that address the sexual exploitation of children over the Internet.

- Given that the vast majority of prosecutions for crimes involving the sexual exploitation of children over the Internet take place at the state level, it is vitally important that state law enforcement officers are trained in investigating these crimes and have access to forensic laboratories.

- Additional resources should be assigned on both the federal and state level to investigate and prosecute these cases. These resources include federal and state law enforcement agents and prosecutors, forensic laboratories and law enforcement and prosecutorial training.

- The use of anonymizers and other encryption methods poses a substantial threat to law enforcement's ability to investigate and bring charges against individuals who create, trade, or otherwise distribute images of child pornography over the Internet. Industry and law enforcement need to work together to develop methods that will allow law enforcement agents to access data related to child sexual exploitation cases while protecting customers' needs to secure their private data unrelated to those cases.

- Currently, NCMEC houses a central database of known images of child sexual exploitation, which includes images found through investigations conducted by U.S. law enforcement, such as the FBI, ICE, and USPIS. It is important that all U.S. law enforcement agencies at the federal and state level have access to this centralized database to consult when investigating crimes involving the sexual exploitation of a child online.

- ISPs that provide connectivity to the Internet do not retain Internet Protocol ("IP") address data linked to a subscriber for the same amount of time. ISPs that provide content also have a wide variety of data retention times for IP addresses and subscriber information.

- It is critically important to investigations involving the online sexual exploitation of children that law enforcement agents are able to access IP address data linked to a subscriber—particularly that information kept by ISPs that provide connectivity to the Internet. Pursuant to 18 U.S.C. § 2703(f), once a law enforcement agent sends a data preservation request to an ISP, the ISP must retain the data described in the request for 90 days, a period which can be extended an additional 90 days if law enforcement requests. Once a preservation request or subpoena has been issued, ISPs should make every effort to respond to law enforcement as expeditiously as possible. Without this information, the investigation is likely to hit a dead end and a child in danger may not be rescued.

- Child pornography investigations often take months to develop, during which time critical data, such as IP addresses linked to a subscriber's account, may be lost if the Internet Service Provider does not have an adequate retention policy.

- Law enforcement agents who testified at the Subcommittee's April 6, 2006 hearing supported a data retention policy of at least one year for IP address information. Due to the fact that harm may be occurring to a child in real-time during an investigation involving the sexual exploitation of children over the Internet, Congress should consider requiring ISPs that provide connectivity to the Internet to retain such IP address information linked to subscriber information necessary to allow law enforcement agents to identify the IP address being used to download or transmit child pornography images and only for so long as necessary to accomplish that purpose.

- When law enforcement agents are able to identify harm that is occurring to a child in real-time, it is essential that they gain immediate access to the IP address and customer information that will allow them to locate and rescue that child. In response to a lawful request, ISPs must provide this information as quickly as possible after the administrative subpoena or other lawful request is received.

- The transmission of a sexual exploitative image of a child over the Internet is a borderless crime because it cuts across state, federal and, in many cases, international jurisdictions. Federal and state law enforcement in the U.S. should consider implementing the Child Exploitation Tracking System, or "CETS," developed by Microsoft and the Royal Canadian Mounted Police, to enhance communication about ongoing investigative subjects in cases involving the sexual exploitation of children between and among U.S. state and federal law enforcement agencies. This program provides a platform for law enforcement agencies to track investigations that are being conducted across the country. This system also enhances the information-sharing critical to these types of investigations as well as reduces the likelihood of unnecessary duplicative efforts. Currently, CETS is being used by Canadian law enforcement officers throughout the territories, and the U.K., Spain, and Italy are beginning to implement this program among their law enforcement agents.

- The current reporting statute for ISPs, 42 U.S.C. § 13032(B)(1), requires "electronic communication service" providers or "remote computing service" providers to report any "apparent" images of child pornography to NCMEC's CyberTipline. Under the statute, it is ambiguous whether cellular phone carriers, social networking websites, and web hosting companies are required to report into the CyberTipline.

- Congress should consider amending 42 U.S.C. § 13032(B)(1) to include mandatory reporting into the CyberTipline for cellular phone carriers, social networking websites, and web hosting companies.

- Currently, 42 U.S.C. § 13032(B)(4) provides that only providers that are found to have "knowingly and willfully" failed to report an "apparent" image of child pornography will be liable for civil penalties. To date, there have been no federal prosecutions under this statutory scheme.

- Congress should consider ways to ensure that all ISPs are proactively searching for and promptly reporting the images of apparent child pornography on their networks.

- Internet Service Providers should develop best practices and technology that will allow them to proactively search their networks and systems in order to identify the transmission of apparent child pornography images, including those transferred by peer-to-peer networks. Such proactive efforts should not expose these companies to potential liability under the current reporting requirements

found in 42 U.S.C. § 13032, criminal liability under 18 U.S.C. § 2252 et seq., or other criminal and civil liability pursuant to Department of Justice antitrust enforcement actions. We recommend that the Department of Justice provide ISPs with guidance on these points to ensure that ISPs continue to cooperate with law enforcement agents on these investigations. These guidelines should also permit ISPs to perform proactive measures on their networks to block images of child pornography and, if the ISP is conducting such measures and blocking child pornography images on their networks, provide assurance to the ISP that they are not in violation of the crimes they are trying to prevent, such as possession and distribution of child pornography images.

- Social networking websites are not enforcing their Terms of Use as vigilantly as they could and, thus, sexual predators are using these websites to find potential victims.

- Social networking websites must take proactive steps to start cross-referencing state sex offender registry lists with those individuals that have profiles on their site, and notify law enforcement immediately of their findings for further investigation. States should consider enacting legislation, such as that proposed in the Commonwealth of Virginia, to require sex offenders to provide their email address when registering as a sex offender so that social networking websites can use the registries to block those offenders from their websites.

- Digital currencies are being used more frequently on commercial child pornography websites and provide another layer of anonymity to the purchaser and seller of these materials. Digital currencies on the Internet are not regulated anywhere in the world.

- The U.S. Department of Treasury and the U.S. Department of Justice should propose legislation to Congress aimed at providing effective controls over the burgeoning digital currency industry over the Internet.

- According to the Internet Watch Foundation ("IWF") in the United Kingdom, approximately 50 percent of the child pornography content the IWF is discovering on the Internet appears to be hosted in the U.S. It is possible that this content may appear to be hosted in the U.S. but in fact is re-routed from another hosting company outside of the U.S. Currently, there is no registration requirement in the U.S. for web hosting companies and thus, it is difficult to know how many companies in the U.S. are hosting content over the Internet. It would benefit law enforcement investigations as well as provide uniformity in the number of web hosting companies that report to the CyberTipline if a registry for web hosting companies was created in the United States.

- U.S. law enforcement investigations have uncovered instances where obvious child pornography domain names were registered with a domain registry company based in the U.S. It would benefit U.S. law enforcement's effort to combat child

pornography over the Internet if domain registry companies registered with an international body and a set of best practices were developed for domain registry companies.

- The IWF provides a valuable service to ISPs in the U.K. by identifying child pornography websites to ISPs and the ISPs in turn block access to the sites identified by the IWF. In September 2006, NCMEC announced that they would be working with law enforcement and the ISPs to provide a similar function to the IWF. Under this initiative, NCMEC will work with law enforcement agents to identify websites that are not the subject of a current investigation. ISPs that report into NCMEC will be advised of these websites and should block them.

- Currently, NCMEC and the IWF do not share with each other the lists of child pornography websites that each has identified. Both organizations should do so and, if NCMEC requires statutory authority both to share and receive these lists, Congress should consider enacting such legislation.

- ISPs in the United States should be encouraged to employ technology that allows them to block customer access to URLs containing child pornography images. In the U.K., ISPs and mobile phone companies use this technology to block a customer's attempt to connect to certain URLs identified by the IWF as containing child pornography, regardless of where such websites are hosted.

- The Department of Justice should explore working with NCMEC and its counterparts in international law enforcement to create a central database of website addresses and URLs that have been identified as containing images of child pornography. This central database should be continuously updated by the member countries as additional websites and URLs containing child pornography are identified, and these URLs and addresses should be shared with the ISPs of the member countries so that they may block access to those websites.

- The proliferation of child pornography images on the Internet demonstrates this is a global problem, with the content originating in many different countries. Under the current U.S. code, NCMEC is not explicitly authorized to transmit images of child pornography to international law enforcement agencies. In order to facilitate the sharing of images among law enforcement necessary to identify and rescue children throughout the world, Congress should consider adding a provision to 42 U.S.C. § 13032, 42 U.S.C. § 5573, and other relevant statutes to explicitly authorize NCMEC for law enforcement purposes to share images contained in their database to law enforcement agents in other countries.

- Many pedophiles collect "series" of child pornography images and these images are circulated around the world thousands if not millions of times. Further, pedophiles tend to build large collections of sexually exploitative images of children. It is critical that every feasible measure be taken to stop the transmission of these images.

- Some ISPs are taking proactive measures to block known images of child pornography that they become aware of on their network. This is done by taking a hash mark (digital fingerprint) of the images; however, an ISP's database of known images is only a fraction of the size of NCMEC's database.

- Under the current U.S. code, NCMEC is not explicitly authorized to share information embedded in the digital fingerprint of an image to any ISP reporting into the CyberTipline. Congress should consider amending 42 U.S.C § 13032, 42 U.S.C. § 5773, and other relevant statutes to grant explicit authorization for NCMEC to share the digital fingerprint of an apparent image of child pornography to ISPs that report into the CyberTipline. This will enable ISPs to block access to many more identified images of child pornography.

- ISPs that report into the CyberTipline for law enforcement purposes should be granted a limited safe harbor provision for the "transmission" or "possession" of child pornography as it pertains to receiving digital fingerprint information from NCMEC and performing proactive measures on its network to block images of apparent child pornography.

II. Background

Crimes involving the sexual exploitation of children, including child pornography, have long been a challenge for U.S. law enforcement. Until the advent of the Internet, the primary obstacle facing law enforcement agents investigating these cases was the sheer number of "purchasers" and "possessors" in the U.S. In addition, most of the producers of child pornography images were outside the United States, further hindering law enforcement agents' investigations and prosecutions.

Despite these challenges, by the late 1980s, U.S. law enforcement was able to significantly reduce the creation and distribution of child pornography through the mails and other commercial avenues. These investigations were led by the U.S. Customs Service and the U.S. Postal Inspection Service, who focused their efforts on vigilantly monitoring the U.S. mail system and engaging in aggressive border inspection of incoming materials. Law enforcement officials attributed their success, in large part, to the fact that those who desired to purchase or trade child pornography images were constricted to a limited, and largely underground, distribution network. Up until the mid-1990s, the primary means of transporting and obtaining images of child pornography was through the mail system; individuals who sought to obtain child pornography images typically did so by responding to mail solicitations and advertisements in the back of magazines or newspapers. The stigma attached to this criminal conduct also limited the commercial sources for child pornography because the "community" of pedophiles did not have an easy way to communicate and distribute images among themselves. In addition, most producers did not have the capability of developing photographs or film

within the privacy of their home and were forced to go to brick and mortar businesses, further heightening the chances of law enforcement agents intercepting the images.

Law enforcement's success in curbing child pornography during the 1980s was significantly bolstered by several Supreme Court decisions and by subsequent congressional legislation. In 1982, the U.S. Supreme Court held in New York v. Ferber[1] that possession of child pornography is not entitled to First Amendment protection and may be criminalized. In Ferber, the Court recognized that the use of children as subjects of pornographic material has long term harmful effects on the physiological, emotional and mental health of the child. The Ferber decision triggered the passing of additional state and federal criminal statutes which criminalized possession, manufacturing, and distribution of child pornography. Eight years later, the Supreme Court held in Osborne v. Ohio[2] that mere possession or viewing of child pornography may be criminalized.

Although considerable progress was made in preventing the distribution of child pornography images through the mails, by the 1980s and early 1990s, many pedophiles were already experimenting with the precursors to the World Wide Web,[3] "newsgroups" and Internet Relay Channels ("IRC"), in order to communicate and facilitate buying, selling and trading of images. At that time, U.S. law enforcement agents were not yet focused on these methods of communication and distribution of child pornographic materials. The growing reliance on the Internet, as well as the development of digital cameras, resulted in a significant increase in the amount of child pornography images and in the number of participants in this criminal enterprise. There are three main reasons for this: (1) the Internet provides an anonymous and quick method of transporting images, particularly since broadband was introduced; (2) the Internet provides an anonymous forum for pedophiles to communicate and connect with one another; and (3) digital photographs preclude the need for going to a photography shop to have the photographs developed, hence making the transmission of the images more private.

Although it is impossible to know the exact number of child pornography images on the Internet, to date, the National Center for Missing and Exploited Children's ("NCMEC") Child Victim Identification Program ("CVIP") has reviewed more than six million individual images related to apparent child pornography. NCMEC, as well as various U.S. law enforcement agencies, house a database of known apparent images of child pornography. The CVIP database is comprised, in part, of images submitted by United States law enforcement agencies. The purpose of this database is two-fold. First, the database can be used to determine if a child-victim has already been identified. Second, the database is used by U.S. law enforcement agents and prosecutors as a mechanism to establish whether the image is of a "real" child, as opposed to a virtual image.[4] Currently, NCMEC has been able to identify and, with the assistance of law

[1] 458 U.S. 757 (1982).
[2] 495 U.S. 913 (1990).
[3] Hereinafter, a reference to the "Internet" means the World Wide Web.
[4] In Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002), the U.S. Supreme Court held that only child pornography involving actual children may be considered "child pornography" for purposes of criminal prosecution under 18 U.S.C. § 2252 et seq. Id. at 254. Therefore, prosecutors in the U.S., unlike the rest of

enforcement agents, rescue 880 minor children who were being subjected to sexually exploitative conduct.[5]

Just as the number of child pornography images available on the Internet has increased, the number of websites offering child pornography images is multiplying. Ernie Allen, President and Chief Executive Officer ("CEO"), of NCMEC, testified at the Subcommittee's April 4, 2006 hearing, that NCMEC estimates there are 100,000 websites offering images of child pornography. Arnold Bell, who currently heads the FBI's Innocent Images Unit, which is charged with investigating child pornography and child exploitation crimes on the Internet, testified that a search on Google using a single search term revealed 130,000 child pornography websites. The number of reports to NCMEC's Cybertipline,[6] the entity created by Congress that is responsible for gathering reports from Internet Service Providers and the public regarding Internet child pornography, further demonstrates the growth of the sexual exploitation of children over the Internet. In its first year of operation in 1998, the Cybertipline received 4,800 reports of child pornography. Since then, reports to the Cybertipline have increased almost 400 percent to approximately 385,000 total complaints. In 2004, the Cybertipline processed 112,000 reports. Currently, the Cybertipline handles an average of 1,500 reports a week of Internet child pornography.[7]

While the explosion in the number of reports to the Cybertipline is a reflection of the growth in online child pornography, that number necessarily underestimates the number of child pornography images that exist on the Internet as not all Internet Service Providers in the United States report to NCMEC the apparent images of child pornography they find on their systems. In fact, only 303 of the hundreds of ISPs operating in the United States are currently registered with and reporting to the Cybertipline. In addition, current federal law does not mandate that every entity that uncovers apparent images of child pornography on its networks or systems report them to NCMEC. Under 42 U.S.C. § 13032, only those companies who provide "electronic communication service[s]" or "remote computing service[s]" must report "known" images of "apparent" child pornography to the Cybertipline. Therefore, credit card companies, social networking websites, and cellular carriers who discover images of child pornography on their networks are not included in the mandatory reporting requirements of the statute, nor are they subject to any separate statutory reporting

---

the world, have the burden of showing that an image is one of an actual child. Hence, the identification of minor victims in child pornography images is critical to proving a criminal violation in these cases.

[5] In addition to NCMEC, Interpol, which houses a database of all known images of child pornography world-wide (including NCMEC's images), also attempts to identify victims in the images. Interpol seeks to identify the country in which the child is from and then forwards the image and any information it can uncover from the image to the law enforcement agency in that country in the hopes that the child may be rescued. Like NCMEC, Interpol also tries to determine if a previously unidentified image of child pornography has been discovered. As of May 2006, Interpol had assisted in identifying and rescuing 426 victims of online child pornography from the 475,899 images it has collected in its database.

[6] The Cybertipline is primarily supported by funding from the Department of Justice. In addition, it receives some funding from the Departments of Homeland Security and State.

[7] Ernie Allen Testimony, Subcommittee on Oversight and Investigations, "Sexual Exploitation of Children over the Internet: What Parents, Kids and Congress Need to Know about Child Predators," April 4, 2006.

requirements. Also, under current law, ISPs and other related Internet providers are under no duty to proactively review or search their networks for images of apparent child pornography. Instead, current law only requires that they report apparent images of child pornography to NCMEC once they are made aware of them or otherwise discover them.

Not only has the Internet contributed to an increase in child abuse images, it has also influenced the content of those images. According to law enforcement agents, the vast proliferation of child pornography images has driven a demand for "new" images of child abuse, thereby perpetuating the sexual abuse of children. Experts in Internet child pornography cases have explained that constant exposure to pornographic images of children on the Internet desensitizes the viewer. This leads the viewer to seek more violent images of children being sexually abused and also to seek images of younger victims in order to gratify his desires. Consequently, NCMEC reported that 39 percent of those persons caught with images of child sexual abuse had images of children younger than six-years-old. In addition, NCMEC found that 19 percent of those persons arrested on child pornography charges between July 2000 and June 2001 possessed images of children younger than three-years-old.

As well as providing ready access to an increased number of child pornography images, the Internet has provided a new way for child predators and pedophiles to access their victims. Every day, more teenagers and children are online. The Pew Internet & American Life Project found in 2005 that 21 million teenagers now use the Internet, with 50 percent online daily. Teenagers not only "surf" the Internet, but they communicate with people they meet online through email, Instant Messaging services, and personal webpages on social networking websites such as MySpace, Xanga, or Facebook. Child predators often use these forms of communication to "groom" their potential child victims. By communicating with children regularly over the Internet, the child predator is able to befriend the child and make him or her comfortable with sharing personal information with someone he or she has not met face-to-face. Eventually, these communications can become sexual in nature, often as a precursor to asking the child to meet the predator or to share sexual images of herself or himself. In fact, NCMEC released a study in August 2006 that found that one in seven children from the ages of 10 to 17 years-old report that they have received a sexual solicitation from someone they met on the Internet.

Experts, including noted forensic pediatrician Dr. Sharon W. Cooper, agree that the physical and psychological harm suffered by the victims of Internet child pornography continues long after the abuse ends.[8] In large part, this is because the image on the Internet exists in perpetuity, essentially re-abusing the child each time it is traded or sold and viewed by another pedophile. The image, which is essentially a crime scene, can never be destroyed or removed from the Internet, even if the perpetrator eventually goes to prison. The result is that the child is continually re-victimized each time someone

[8] Dr. Cooper and other physicians and experts in child sexual exploitation authored a treatise on child sexual exploitation and addressed the impact of sexual exploitation on child victims throughout their lives. *See* Sharon W. Cooper, Richard J. Estes, et al., Medical, Legal, & Social Science Aspects of Child Sexual Exploitation A Comprehensive Review of Pornography, Prostitution, and Internet Crimes, 2005.

clicks on his or her image, forwards it, or distributes it. This is the reason why victims of Internet child pornography like Masha Allen, a child victim who testified at the Subcommittee's May 3, 2006 hearing, have pleaded for every effort to be made to prevent the distribution of child pornography images. As Ms. Allen stated in her testimony, the thing that upset her most about the abuse she suffered is that her images would be on the Internet "forever."

The prevalence of online child pornography also has a distinct psychological impact on those who collect and possess it. According to psychologists who study the issue, individuals collect child pornography not only for sexual gratification but as a "plan for action."[9] A study conducted by Dr. Andres C. Hernandez and published in a poster presentation entitled "Self Reported Contact Sexual Offenses by Participants in the Federal Bureau of Prisons' Sex Offender Treatment Program: Implications for Sex Offenders" supports the notion that viewing child pornography is likely to lead to contact offenses involving a child. The study showed that, of the inmates who elected to participate in the Federal Bureau of Prisons Sex Offender Treatment Program, 76 percent of those who were convicted on charges related to Internet sex crimes, such as possession of child pornography or luring a child, had also committed sexual contact offenses against children. This conclusion was based on polygraph examinations of offenders who chose to enroll in Dr. Hernandez's program. This link between viewing or possessing child pornography and molesting a child has been demonstrated in other studies as well, including one conducted by the United States Postal Inspection Service beginning in 1997. This study found that 33 percent of the 2,433 individuals arrested by USPIS agents since 1997 for using the U.S. mail and the Internet for the sexual exploitation of children had molested children. These findings are alarming and lend credence to the notice that exposure to images of child pornography can, in fact, create child molesters, and hence, result in more child-victims.[10]

Of additional concern is that commercial Internet child pornography has become a lucrative and growing business. Although it is impossible to pinpoint the revenue generated by an illegal business, such as commercial child pornography, some estimates indicate that commercial child pornography may generate billions of dollars a year in revenue.[11] To evade detection by law enforcement agents, the payment schemes employed by commercial child pornography websites are increasingly complex and involve the use of digital and electronic currencies and other forms of barter. Those individuals who sell child pornography images often set up fictitious businesses in order to obtain a merchant account for credit card processing. The technology supporting these websites is equally sophisticated. It is not unusual for websites to be registered using

[9] Dr. Sharon Cooper Testimony, Subcommittee on Oversight and Investigations, "Sexual Exploitation of Children over the Internet: What Parents, Kids and Congress Need to Know about Child Predators," April 4, 2006.

[10] A polygraph study currently being conducted in the Netherlands of convicted sex offenders further supports Dr. Hernandez's finding that a link exists between possessing child pornography images and committing contact crimes against children.

[11] *See* Cassell Bryan-Low, "Dangerous Mix: Internet Transforms Child Porn Into Lucrative Criminal Trade — Company in Belarus Collected Millions From Pedophiles; A Landmark Prosecution — Agent's Rendezvous in Paris," Wall Street Journal, Jan. 17, 2006, at 1.

fictitious names and to use servers in several different countries to host images, thereby making it extremely difficult for law enforcement agents to identify the responsible individuals. Even so, according to several reports published quarterly by the Internet Watch Foundation ("IWF")[12] in the United Kingdom, the United States appears to be hosting a majority of the child pornography content on the Internet. Law enforcement agents believe that this may be due to the fact that the United States has some of the fastest and most advanced Internet connectivity in the world, making U.S. servers especially appealing to commercial child pornography operators looking for servers to host their content. It is unclear, though, whether all of the websites that the IWF claims are hosted in the U.S. are, in fact, hosted here or whether a proxy server is being used. Currently, web hosting companies in the U.S. do not typically review any of the content on their servers nor do they report into NCMEC's Cybertipline on a regular basis.[13]

Law enforcement agents at both the state and federal levels are working to combat the proliferation of sexually exploitative images of children over the Internet. In the U.S., there are four primary law enforcement agencies which investigate the sexual exploitation of children over the Internet. These agencies are: (1) the Federal Bureau of Investigation ("FBI"); (2) Immigrations and Customs Enforcement ("ICE"); (3) the U.S. Postal Inspection Service ("USPIS") and (4) the Internet Crimes Against Children ("ICAC") Task Forces. Currently, agents from each of these law enforcement agencies as well as the U.S. Marshals Service are assigned to NCMEC and assist in investigating the tips reported to the Cybertipline. All of these law enforcement entities have jurisdiction over cases involving the sexual exploitation of children; however, each has a primary mission and jurisdiction that dictates what types of cases the agents will work.

Within the FBI, the Innocent Images National Initiative is responsible for investigating Internet child pornography cases. Fifteen agents and 22 analysts are assigned to this unit, based in Calverton, Maryland. The FBI also has agents in field offices around the country that may be assigned a child sexual exploitation case, however, no field agents exclusively work on child sexual exploitation cases over the Internet. For cases with an international nexus, the Cyber Crimes Center of ICE has jurisdiction. Currently, 10 to 12 agents within the CyberCrimes Center are dedicated to investigating exclusively child exploitation crimes, and in the field, there are the equivalent of 221 ICE agents dedicated to Operation Predator cases, an initiative

[12] The Internet Watch Foundation ("IWF") and its "hotline" in the United Kingdom are similar to the NCMEC and the Cybertipline in the United States. Like the NCMEC, the IWF is responsible for gathering reports from ISPs and the public of Internet child pornography. However, the IWF, which partners with the U.K. Home Office and Department of Trade and Industry, receives most of its funding from U.K. Internet Service Providers, cellular or mobile companies, and the telecommunications industry. In addition, the IWF operates a "notice and takedown" system, by which it distributes the Uniform Resource Locator, or "URL," of Internet child pornography images to the Internet Service Providers in the U.K. The providers then use various forms of technology to "block" the URLs of child pornography images, thereby preventing the public from accessing those images from the United Kingdom.

[13] Under 42 U.S.C. § 13032, an "electronic communication service provider" is required to report "known" and "apparent" images of child pornography to the Cybertipline. It is unclear if web hosting companies would fall under the definition of "electronic communication service provider" and thus, may have no statutory obligation to report to the Cybertipline. NCMEC has informed Committee staff that a few web hosting companies do voluntarily report into the Cybertipline.

developed by the Department of Homeland Security and ICE to identify, investigate, and arrest child predators. Finally, 35 postal inspection agents are dedicated to investigating Internet child pornography cases that involve the use of the mails on a full-time basis.

On the state level, the ICACs are federally funded and trained state and local police officers dedicated to investigate crimes related to the sexual exploitation of children over the Internet. The ICACs are funded primarily through the Department of Justice's Office of Juvenile Justice and Delinquency Prevention ("OJJDP") and work cooperatively with their counterparts in federal law enforcement. During fiscal year 2006, Congress appropriated $14,315,00 to OJJDP for ICAC Task Force operations. In addition to ICAC trained officers, there are also many state and local law enforcement officers that work on online child sexual exploitation cases, both in proactive and reactive investigations.

Recently, the Department of Justice ("DOJ") announced a series of initiatives aimed at investigating and prosecuting the sexual exploitation of children over the Internet. In February 2006, Attorney General Gonzales announced "Project Safe Childhood." The goal of the project is to coordinate efforts between state, local, and federal law enforcement authorities when investigating Internet crimes against children. On May 17, 2006, Attorney General Gonzales announced that Project Safe Childhood would be implemented on a national level. The initiative requires each United States Attorney to designate a Project Safe Childhood coordinator within two weeks and to begin meeting with local partners to develop a plan for their district within 90 days. In addition, U.S. Attorneys must partner with their local ICACs and federal law enforcement agents in order to increase federal involvement in child pornography cases and to train state and local enforcement and educate local communities.

On April 21, 2006, DOJ submitted proposed legislation to Congress to amend 42 U.S.C. § 13032. DOJ's proposed amendment would triple the fines imposed on electronic communications services providers who knowingly and willfully fail to report to NCMEC's Cybertipline, as required by 42 U.S.C. § 13032. Under the proposed legislation, delinquent providers would be assessed $150,000 for an initial violation and $300,000 for each subsequent violation. In addition to increasing fines for those who knowingly and willfully fail to report, on May 15, 2006, DOJ proposed a second piece of legislation that would impose fines on providers who negligently fail to report. The current statute requires that the provider "knowingly and willfully" failed to report. Under the proposed legislation, the provider would be fined $50,000 for the initial, negligent failure to report and $100,000 for each subsequent violation. Under the current statutory scheme, DOJ has never prosecuted a provider. Neither proposal was enacted by the House or Senate.

III. **The Subcommittee Investigation**

In January 2006, the Subcommittee on Oversight and Investigations initiated its investigation of the sexual exploitation of children over the Internet to examine the scope of the problem; the approach of law enforcement; the entities involved; and ways to

prevent the proliferation of child pornography on the Internet. The investigation was prompted by an article in The New York Times by Kurt Eichenwald entitled "Through his Webcam, a Boy Joins a Sordid Online World." The article featured the story of Justin Berry, now a 19-year-old young man. Beginning at the age of 13-years-old, Justin was repeatedly victimized by child predators who contacted him over the Internet when they saw his image on a webcam, which he had received as a free promotional gift to subscribers of Earthlink. In addition to describing the abuse he suffered at the hands of the individuals whom he met online, Justin also described how some of these individuals encouraged him and even assisted him in developing and operating commercial pornography websites featuring sexual images and videos of Justin. In that article, Justin also stated that he provided prosecutors in the Department of Justice's Child Exploitation and Obscenity Section ("CEOS"), and the FBI with specific information about those individuals involved in the commercial child pornography business, including the names of the individuals who helped him host the websites and process payments. As a result of the information Justin voluntarily provided to DOJ, he was granted immunity. According to the article, Justin was concerned about how DOJ and the FBI handled the information that he provided to them about a commercial child pornography enterprise.

Based on the Committee's jurisdiction over matters related to the Internet, telecommunications and consumer safety, Committee leadership instructed staff to review U.S. law enforcement efforts to combat online child pornography, the role of NCMEC as a conduit between law enforcement and private industry, and how private industry is responding to this threat against children over the Internet. As the extent of this criminal activity became clear, the investigation was expanded to include all methods by which the Internet was used in the sexual exploitation of children.

A. **Law Enforcement Efforts to Combat the Sexual Exploitation of Children Over the Internet**

In addition to investigating Justin Berry's allegations regarding the Justice Department and FBI, the Committee also began investigating information reported by Kurt Eichenwald with regard to the ease with which he could locate images of child sexual abuse on the Internet and the commercial enterprises that are associated with child exploitation over the Internet. To that end, Committee staff met with and interviewed various law enforcement agencies and other groups to gain a better understanding of the scope of the problem and how they are working to combat the proliferation of sexually exploitive images of children over the Internet. In particular, Committee staff met with officials from NCMEC and visited NCMEC's offices in Alexandria, Virginia, in order to better understand how the Cybertipline operates.

Committee staff also visited the offices of the federal law enforcement agencies that are responsible for investigating the online exploitation of children, including the FBI's Innocent Images unit and ICE's Cyber Crimes Center, and met with agents and officials from the U.S. Postal Inspection Service. Committee staff learned that while there is an active federal law enforcement effort to combat Internet child pornography, the vast

majority of investigations — approximately 70 percent — take place at the state or local level. For this reason, Committee staff also interviewed several state ICAC Task Force investigators.

Interviews and meetings with law enforcement officials and agents revealed several key factors which have contributed both to the proliferation of child abuse images on the Internet as well as the obstacles law enforcement agents face when they try to identify the individuals who possess and distribute these images. First, and perhaps most daunting, is the number of child abuse images on the Internet. As mentioned previously, United States law enforcement estimates that there are approximately 3.5 million known child pornography images online. In addition, the individuals who trade and distribute child pornography images use sophisticated technology and other means to evade identification by law enforcement agents. For example, law enforcement agents said that individuals who download images can use "anonymizers" or encryption technology which makes it difficult to find the individuals, much less prove that they possessed or downloaded the images. Law enforcement agents also stated that most Internet Service Providers often do not retain Internet Protocol, or IP, address data for a sufficient period of time. Without this data, law enforcement agents are unable to identify the individual at a certain IP address who has downloaded or distributed child pornography. Further, law enforcement agents are concerned that the response time of ISPs to law enforcement inquiries or subpoenas seeking the identity of a customer assigned to a particular IP address varies and is not always timely. Dr. Frank Kardasz, a member of the Arizona ICAC Task Force, testified that a two-day response time to law enforcement subpoenas for IP address information would be ideal.

Law enforcement officials also explained that the payment schemes used by commercial child pornography websites are becoming increasingly complex and sophisticated, again, as a method to evade detection. One example cited by law enforcement officials and by NCMEC is the increasing use of digital currencies as a method of payment on commercial child pornography websites. Payment by digital currencies makes it more difficult for law enforcement agents to trace the payment, and thus, the source.

In addition to examining how law enforcement officials investigate and prosecute those who exploit children over the Internet, Committee staff reviewed and analyzed existing federal law with regard to criminal penalties for possession, creation, and distribution of child pornography. A review of federal and state law showed that while penalties for federal charges can be quite severe — for example, the federal sentence for distribution of child pornography is up to 20 years, with a five year minimum mandatory sentence, per image — there is great disparity among state penalties for crimes involving child pornography. Because the vast majority of these online child sexual exploitation cases are prosecuted on the state level, it is imperative that all states consider adopting strict sentencing schemes for these crimes and laws that clearly address the online environment in which these crimes are now committed. For example, all states should consider adopting laws that make clear that sexual solicitation of a person believed to be a minor online is a felony offense, with automatic jail time. In addition, Committee staff

learned that possession of child pornography currently is not a felony offense in all 50 states. This needs to be considered immediately by the states.

The Subcommittee on Oversight and Investigations held its first two days of hearings on the issue of sexual exploitation of children over the Internet on April 4 and 6, 2006. This hearing, entitled "Sexual Exploitation of Children Over the Internet: What Parents, Kids and Congress Need to Know about Child Predators," focused on explaining the scope of the problem, U.S. law enforcement's approach to investigating and prosecuting child pornography crimes, the impact of sexual exploitation on its victims, and efforts by Internet safety groups to educate parents and children.

On April 4, the witnesses included Mr. Ernie Allen of NCMEC; a child victim, Justin Berry; The New York Times reporter Kurt Eichenwald; Dr. Sharon Cooper, a forensic pediatrician specializing in child sexual exploitation; and Ms. Teri L. Schroeder and Ms. Parry Aftab, advocates for Internet safety from i-Safe and Wired Safety, respectively. In addition, Mr. Kenneth Gourlay of Michigan, whom Justin Berry had identified as the man who first molested him after meeting him online, appeared pursuant to Committee subpoena. Mr. Gourlay asserted his Fifth Amendment right against self incrimination and refused to testify in response to the Subcommittee's questions.[14]

Testifying on April 6 were Mr. William E. Kezer, Deputy Chief Inspector, and Mr. Raymond C. Smith, Assistant Inspector in Charge, on behalf of the U.S. Postal Inspection Service; Dr. Frank Kardasz, Phoenix Police Department Sergeant, and Mr. Flint Waters, Lead Special Agent of the Wyoming Division of Criminal Investigation, on behalf of the Arizona and Wyoming ICAC Task Forces, respectively; Mr. John P. Clark, Deputy Assistant Secretary, and Mr. James Plitt, Director of the Cyber Crimes Center, on behalf of the Department of Homeland Security, Immigration and Customs Enforcement; and Mr. Greer Weeks, an expert in state child pornography laws and sentences. In addition to these witnesses, in order to better understand the approach of law enforcement to investigating and prosecuting crimes involving the online sexual exploitation of children, the Committee requested that the Honorable Alice S. Fisher, the Assistant Attorney General for the Criminal Division, and Mr. Andrew Oosterbaan, Chief of the Child Exploitation and Obscenity Section, testify on behalf of the Justice Department, and that Mr. Raul Roldan, Section Chief, Cyber Crime Section of the Cyber Division, and Mr. Arnold E. Bell, Unit Chief, Innocent Images Unit, testify on behalf of the FBI. In lieu of the requested witnesses, the Department of Justice and the FBI designated Mr. William Mercer, Principle Associate Deputy Attorney General and United States Attorney for the District of Montana, and Mr. Chris Swecker, Acting Assistant Executive Director of the FBI, to testify on their behalf. Subsequently, at the Committee's hearing on May 3, 2006,

[14] Immediately following the hearing, Mr. Gourlay's residence was searched pursuant to a search warrant obtained by the Michigan Attorney General. Just one month later, on May 15, 2006, Mr. Gourlay was arrested on 10 felony counts related to the allegations made by Justin Berry during the Subcommittee hearing, including Criminal Sexual Conduct, Child Sexually Abusive Activity, Using a Computer to Commit a Crime, Distribution of Child Sexually Abusive Activity and Accosting a Child for Immoral Purposes. On September 19, 2006, Mr. Gourlay was charged with 18 additional felony counts of Criminal Sexual Conduct. The charges are currently pending before a Michigan state court.

Ms. Fisher, Mr. Roldan, and Mr. Bell appeared before the Committee and testified about their departments' approach to sexual crimes against children over the Internet.

On May 3, 2006, the Subcommittee held a third day of hearings dedicated to law enforcement's approach to online child pornography crimes, specifically, the efforts of the FBI and Department of Justice. As mentioned previously, testifying on behalf of the Justice Department was Ms. Fisher and, on behalf of the FBI, Mr. Roldan and Mr. Bell. The witnesses described recent initiatives by the Justice Department to combat Internet crimes against children, including Project Safe Childhood, prosecutions by the Child Exploitation and Obscenity Section ("CEOS") of DOJ, and FBI investigations. In addition, Ms. Fisher, Mr. Roldan, and Mr. Bell were asked to address their departments' action with respect to charges made and information provided by Justin Berry. In large part, the witnesses testified that they were not able to respond to questions about Mr. Berry's allegations due to ongoing investigations related to his case.

In addition, the Subcommittee also heard testimony from Ms. Masha Allen, a 13 year-old girl, who was adopted from Russia when she was five-years-old by a divorced man from Pittsburgh, Pennsylvania, named Matthew Mancuso. Masha was accompanied at the hearing by her attorney, James Marsh; her advisor, Maureen Flatley; and, at her request, television news reporter Nancy Grace. From the time she arrived in the U.S. with Mancuso, she was repeatedly sexually assaulted by him and images of her abuse were posted on the Internet by Mancuso. After approximately five years of sexual abuse, Masha was rescued as the result of an undercover Internet investigation by the Chicago Police Department. Mancuso is currently serving a 30 year federal sentence and will then serve a consecutive state sentence on charges related to his abuse of Masha. In addition to describing her harrowing ordeal at the hands of Mancuso, Masha also raised questions about the conduct of the U.S. adoption agencies that worked with Mancuso to place a five-year-old girl with him. The Subcommittee held a hearing on September 27, 2006 to follow-up on Masha's questions and concerns.

The April and May hearings revealed important information about the scope of the problem, law enforcement's efforts to fight it, and the efforts to educate parents and children about the dangers that exist online. In short, the sexual exploitation of children over the Internet is a problem of great urgency. As Mr. Ernie Allen, President and C.E.O. of NCMEC, testified, sexual abuse images of younger children and even toddlers are becoming more prevalent over the Internet. For example, on March 15, 2006, the Department of Justice and ICE announced a bust of an Internet child pornography ring in the United States, Canada, the United Kingdom, and Australia in which the images seized included a live, streaming video of an infant who was less than 18 months old being raped by an adult male.

It is also clear that while both federal and state law enforcement agents are actively pursuing investigations of online child pornography, law enforcement either needs additional resources or better prioritization and organization within their agencies, or both, to allow additional funding for personnel, forensic assistance, and training for state agents. In addition, law enforcement agents explained that the data retention policies of

some Internet Service Providers are inadequate and, in some cases, their failure to retain for a sufficient period of time the information that links an IP address to an Internet customer has prevented law enforcement agents from identifying child predators and rescuing children. For example, Mr. Flint Waters of the Wyoming ICAC testified that, in one case, an ICAC investigator intercepted the transmission over a peer-to-peer network of a video showing the rape of a two-year-old child and was able to trace the video to a computer in Colorado. When the ICAC agent approached the Internet Service Provider, Comcast, to request the customer information for the IP address in Colorado, Comcast informed the agent that it had not retained the customer records for that address. As of the date of the hearing, to Mr. Waters' knowledge, the child in the video had not been identified.

Following the April hearings, Committee staff traveled to the United Kingdom and to Interpol headquarters in France to meet with government, law enforcement, and industry officials to discuss how they are working to combat Internet child pornography. In the United Kingdom, Committee staff met with officials from the United Kingdom's Home Office, the equivalent of the United States Department of Justice; the Department of Trade and Industry; the Internet Watch Foundation; members of the mobile telephone industry; the Internet and telecommunications industries; and child advocates. In addition, Committee staff met with the Chief Executive and Staff of the Child Exploitation and Online Protection Centre ("CEOP"), a new quasi-government organization that partners law enforcement with the business sector, charities, and other organizations. CEOP is dedicated solely to fighting and investigating sexual crimes against children, particularly Internet sex crimes. Committee staff also traveled to Lyon, France to meet with agents from Interpol, the international police organization, in order to learn more about Interpol's database of child abuse images and its efforts to identify and rescue the children abused in these images.

The meetings with British officials and with Interpol revealed important differences between the approach of U.S. law enforcement and its international counterparts. For example, the United Kingdom employs a "notice and takedown" approach in fighting child pornography. Under this approach, which was first implemented by some companies in 2004, Internet Service Providers voluntarily agreed to block access to URLs identified by the IWF as containing images of child pornography.[15] British officials attribute the fact that only .2 percent of websites containing child pornography images are currently hosted in the U.K. — down from 18 percent in 1997 — in part to this blocking approach, whereas the IWF has found that 51.1 percent of websites containing child pornography content are hosted in the United States.[16] According to these officials, in the United States, websites with child pornography are not immediately taken down after law enforcement learns of them; instead, the websites are left up so that law enforcement agents have an opportunity to investigate and prepare charges against the individuals operating the site.

[15] The website of the IWF can be found at www.iwf.org.uk.
[16] Internet Watch Foundation 2006 Half Yearly Report.

A recent proposal by NCMEC supports a dual approach of furthering law enforcement investigations and shutting down the websites. NCMEC, which announced the initiative at the Subcommittee's September 26, 2006 hearing, explained that they are working with law enforcement and the industry to devise a system that is similar to the U.K.'s notice and takedown model. Notably, this approach was suggested by NCMEC after the Committee expressed an interest in setting up a system in the U.S. similar to the IWF's "notice and takedown" approach to child pornography websites. According to NCMEC's proposal, law enforcement agents will first be notified of child pornography websites so that they have the opportunity to investigate the website and gather evidence. Then, if the law enforcement agents agree, NCMEC will forward the Internet address for the website to the ISPs so that the ISPs may block the website on their system. By involving law enforcement from the beginning, the NCMEC approach might avoid an issue faced by those systems that primarily rely on notice and takedown to put an end to the proliferation of online child pornography: child pornography websites move Internet addresses constantly to avoid detection and, if subject to a takedown, simply move their content to a new Internet address. In addition, peer-to-peer systems, rather than websites, are becoming a popular way to trade child pornography images because these systems make it difficult for law enforcement agents to trace and intercept the transmission of images. A notice and takedown approach is largely ineffective against this type of technology.

The cooperation and sharing of ideas among U.S. and international law enforcement, NCMEC, the IWF, and other international groups must continue so that the fight against online child pornography can be won. NCMEC's recent notice and takedown proposal is a prime example of how law enforcement can improve its tools and methods by learning from the experience of other countries. The experience of foreign industry in preventing child pornography can also be a resource for U.S. businesses. In the United Kingdom, British telecommunications companies and some mobile telephone companies that provide connectivity to the Internet have developed systems intended to prevent their customers from connecting to child pornography websites.

B. The Role of Internet Service Providers and Social Networking Websites in Combating the Sexual Exploitation of Children Over the Internet

In order to examine the role of the U.S. Internet Service Provider industry in the fight against child pornography, the Subcommittee convened two days of hearings on June 27 and 28, 2006 entitled "Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites." The Internet Service Providers testifying at this hearing included representatives from America Online ("AOL"), Microsoft, Google, Yahoo, Earthlink, Comcast, and Verizon; the social networking websites included MySpace, Xanga, and Facebook. Commissioner Pamela Jones Harbour of the Federal Trade Commission, and Diego Ruiz, Deputy Chief, Office of Strategic Planning and Policy Analysis, of the Federal Communications Commission, also testified about the role of their agencies in regulating Internet companies.

Also testifying was television news journalist Chris Hansen, who led a multi-part investigative series that aired on Dateline NBC, entitled "To Catch a Predator." The series focused on the activities of child predators on the Internet and showed how actual child predators contacted and groomed individuals they believed were potential child-victims. The individuals that the predators communicated with online were actually adult volunteers for an online watch-dog group, Perverted Justice. The adult volunteers posed online as 13 or 14-year-old children who were home along and receptive to an in-person meeting with an adult whom they had met on the Internet. In his testimony, Mr. Hansen described the online grooming process he observed between child predators and the "children" and noted how quickly the predator would turn the conversation into one overtly sexual in nature. Mr. Hansen also noted that the individuals who were identified and arrested as a result of the series — at the time of the hearing, 98 of whom had been charged criminally — defied characterization. They came from all walks of life and, upon meeting them, many did not seem to be particularly dangerous or suspicious.

The primary issue addressed at these hearings was whether the Internet industry as a whole was doing enough proactively to prevent the transmission of child pornography images over their systems and networks. In addition, the Committee was interested in whether the policies of these companies, particularly the companies who provide content and accept advertising on their websites, clearly prohibited content or advertising that involves the sexual exploitation of children. Each company discussed the measures they take to keep child pornography from being either hosted or distributed over their systems. The type of approach adopted by a company is dictated by several factors including: (1) the type of service provider they are, that is, whether the company provides "content," like Yahoo!, or is primarily a "pipeline," like Verizon; (2) the types of products they offer on their network, such as email, instant messaging ("IM"), news groups, and search functions; (3) the size of their customer base; and (4) the extent to which the company expends resources in both reactive and proactive measures to review its network for violations of the law, its "Terms of Use" or both.

AOL, a content provider with paid subscribers, explained that it creates a "digital signature" of apparent child pornographic images it finds on its network and then collects those signatures in a digital library. Any image files transmitted over AOL's network are compared to the digital library. In this way, AOL can identify and block the distribution of images that it has previously identified as child pornography. Other providers, like Yahoo! and MSN, use filters as well as algorithms in an attempt to identify child pornography images transmitted over their networks and shared through their programs, such as chatrooms.

Network service providers, or "pipelines," like Verizon or Comcast, are in a somewhat different position. Unlike content providers, network service providers mainly provide access to the Internet but do not provide other services like chat, groups, or search functions. At this point, network service providers do not employ the proactive measures that content providers use to identify the transmission of child pornography images over their networks. Whether this is due to legal or technical constraints their

efforts with respect to child pornography images are mostly reactive. As some pipeline providers explained to the Subcommittee, the primary way they discover child pornography images on their networks is by customer reports or complaints, which the pipeline provider then forwards to NCMEC. Pipeline providers also respond to law enforcement agents' requests and subpoenas for customer information.

In addition to their proactive measures, the Internet Service Providers also explained their data retention policies and addressed the announcement of the Department of Justice that it intended to explore with ISPs establishing a uniform data retention policy for the purpose of enhancing law enforcement's investigations of Internet child pornography.[17] As discussed previously, law enforcement agents who testified at the Subcommittee's April and May hearings explained that inadequate data retention policies had prevented them in some cases from identifying individuals who create or distribute child pornography images over the Internet.

While all the Internet Service Providers testified that they report images of apparent child pornography to NCMEC when they discover it on their networks and that they attempt to respond to law enforcement agents' requests and subpoenas as expeditiously as possible, the data retention policies of the ISPs that testified at the hearing vary widely, from 60 days to seven years. Testimony provided at the hearing suggests that the cost of data retention is a determining factor in setting the retention period. AOL, for example, testified that retaining the IP addresses for each user session of every AOL user would cost $44 million per year. Several factors have a bearing on the cost, for example, the types of services offered by the provider, the number of users, and whether the site is free or available only to paid subscribers. However, law enforcement officials have stressed that it is the ISPs that provide connectivity to the Internet which need to retain IP addresses for at least one year for purposes of child pornography investigations.

The operations of social networking websites were also examined at the June hearing. These websites have become increasingly popular in recent years, especially among preteens, teenagers and young adults. Registered users with social networking websites are able to build personal webpages. These webpages often contain personal information about the user, such as where he or she attends school or works, their likes and dislikes, links to their friends' webpages or other websites, contact information, and photographs.

Recently, social networking websites have received a great deal of scrutiny as child predators have used the information on children's webpages to contact them and to groom them in anticipation of meeting them in person. Facebook, MySpace, and Xanga testified about the safeguards they have implemented on their websites.[18] Users of each

[17] At the time of the hearing, AOL retained the data that links an IP address to a customer's name for 90 days; Earthlink for seven years; Comcast for 180 days; Verizon for nine months.

[18] At the time of the hearing, MySpace had 80 million registered users; Xanga had 27 million; and Facebook had more than 8 million. While Facebook, MySpace, and Xanga are each social networking websites, they operate differently with respect to how users can obtain access to the website. MySpace and Xanga are open to the general public. Anyone with Internet access can open a MySpace or Xanga account and build a personal webpage. In contrast, to join Facebook, a user must be validated into one of Facebook's online communities. The communities are largely organized by high schools and colleges, but there are also work

website have the option of making their profiles private, thereby preventing other users from viewing their personal webpage. On MySpace, the "private" setting is the default setting for any user who admits to being under the age of 16 years. Xanga[19] employs similar features which allow a user to restrict their webpage to only other Xanga members or to other designated users, respectively. Xanga has also developed a safety feature, called "Footprints," which, when activated, allows a Xanga member to see the usernames of individuals who have signed into his or her webpage. Similarly, Facebook offers a privacy option which permits the user to determine who can see particular pieces of information about them, including their entire webpage.

In addition to offering a privacy setting, the social networking websites who testified at the June hearing allow their users to report inappropriate content by clicking on links or tabs displayed on the user webpages. Typically, these reports are sent first to the website itself, so that website employees can review the reports and take appropriate action, including terminating the account of a user who has violated the terms and conditions of the website. If the content contained apparent images of child pornography or grooming, each website stated that they report this activity to NCMEC.[20]

The social networking websites also conduct some human and automated review of the content on their webspages, however, more needs to be done to ensure that these

---

networks. In order to be validated, a potential user must have either a ".edu" email address or similar associated with a school or university email domain or, if a high school does not have a domain, high school users can join if they receive an invitation from a college user who graduated from that high school. The high school user who received the invitation will then invite other students from his high school to join; to ensure that individuals who do not have a .edu domain name are, in fact, students at a particular high school, Facebook places a computer code within the invitation email that confirms the individual who joined was the same individual who received the invitation. Additionally, members of Facebook only have access to the profiles of members within their school community. In this way, Facebook users only have access to their school communities. To view the profile of a user outside that community, Facebook members must receive permission from that user. Members of work communities only have access to the profiles of other users who have joined the same regional network they have joined. As MySpace and Xanga are not organized according to work, school, or regional communities, MySpace and Xanga users have access to any other webpage on the website, unless a user has activated a privacy setting that limits access to approved MySpace or Xanga users.

[19] On September 7, 2006, the Federal Trade Commission ("FTC") announced that it had reached a settlement with Xanga related to Xanga's alleged violations of the Children's Online Privacy Protection Act ("COPPA"). The FTC found that Xanga, in violation of COPPA, had improperly collected, used, and disclosed personal information from children under the age of 13 without first notifying their parents and obtaining consent. Under the settlement, Xanga paid a $1 million fine to the FTC.

[20] NCMEC is the designated repository in the United States of all reports of online grooming or child sexual abuse or exploitation, and their link is displayed on several websites in order for users to report abuse. Once a report is received by NCMEC, analysts are available 24 hours a day to review the report and forward it to the appropriate law enforcement agency. Other countries have adopted similar approaches. For example, in the United Kingdom and Australia, many websites display a link to the Virtual Global Taskforce, or VGT. The VGT is comprised of law enforcement agents from Australia, the U.K., Canada, and the U.S., where agents from ICE are members. Internet users can report grooming or online sexual abuse by clicking on the VGT button, or link, displayed on social networking websites or the VGT's website, www.virtualglobaltaskforce.com. The link then takes the user to a reporting page, where he or she is asked to supply certain information such as the webpage where the abuse occurred. The report is then immediately sent to the appropriate country for immediate review and action by law enforcement.

reviews are as effective and aggressive as they can be. For example, at the June hearing, the social networking websites, particularly, MySpace, were asked if they screened their sites for registered sex offenders. At that time, none of the social networking websites conducted any type of screening for sex offenders on their websites. Now, almost six months later, MySpace announced on December 5, 2006 that it was working to develop a technology that will allow it to block convicted sex offenders from accessing MySpace. As the technology has yet to be implemented, its effectiveness remains uncertain. Even so, it seems that the websites primarily rely on their users to ferret out and bring inappropriate content to their attention. As Facebook testified, they believe user reporting works best because Facebook users are best able to recognize individuals who do not belong in their school communities and do not tolerate behavior or content that does not meet the community's standards. While Facebook is unique in that its users webpages are organized according to high school, college, or regional communities and only available to other users within the same community, Xanga also found that its reporting or "flagging" system has proved reliable in identifying child pornography or other inappropriate content.

Despite these safeguards, children's webpages on social networking websites are still vulnerable to child predators as the success of the safeguards largely depends on a child's ability to recognize a dangerous situation, and report it, or to affirmatively activate the safeguards and privacy settings. The search functions of a website also pose a risk to children's safety online. While Xanga and Facebook do not permit its members to search other member's webpages for personal characteristics, such as height, sex, or interests, MySpace users can search member profiles for a variety of factors including sex, age, marital status, body type, and interests. Though the webpages of MySpace users who are under age 16 have a default privacy setting and, even if that setting is deactivated, they are available only to other users under the age of 18, child users are still at some risk because the system can easily be manipulated by users who lie about their age.[21] It takes only minutes to search for and find children who are under 16-years-old on MySpace. For example, Committee staff did a search on MySpace for persons 4'11" or shorter. This simple search uncovered numerous underage users who accurately stated their height in their profile, but who over-reported their age, a common tactic by underage users to evade the MySpace age restrictions.

Although all the social networking sites testified that they have been unable to develop a viable age verification system to weed out underage users, it appears that with some basic search techniques and development of more refined search algorithms, these companies should be able to detect underage users and those violating their Terms of Use in a more effective fashion. The lack of effective methods for protecting the adolescent membership of these websites, or limiting the websites to adults only, necessarily means that children are placed at risk of exposure to child predators. Social networking websites could require a verifiable credit card in order to confirm the age of the user, however, credit card companies have resisted allowing their systems and databases to be used for such confirmation without a purchase first taking place.

[21] MySpace does not permit users who under the age of 18-years-old to specifically browse for users who are 16-years-old or younger. In addition, adults can never browse for users who are 18-years-old or under.

In addition, children often are not able to accurately assess the risk presented by revealing personal information and communicating with individuals they meet in an online community. Detective Frank Dannahey of the Rocky Hill, Connecticut Police Department testified at the Subcommittee's June 28 hearing that children's personal information was often easily available or readily volunteered on the MySpace webpages he reviewed while conducting an experiment on Internet safety. This personal information included where the child lived, worked, the child's full name and date of birth, and cellular and home telephone numbers. According to Detective Dannahey, teenaged users of social networking websites are often very trusting of the people they meet online and do not perceive them as strangers but as friends. For this reason, teenagers are not able to recognize when they are sharing personal information that might identify them to a child predator. These characteristics necessarily undermine safeguard systems that depend on a child's ability to recognize and report inappropriate content.

The risk posed to children by predators who are intent on communicating with them and befriending them online demands that Internet Service Providers and social networking websites take an aggressive approach in developing safeguards to protect children. Already, since Committee staff began meeting with the ISPs and social networking websites early in 2006, these companies have implemented several improvements to their systems. For example, when Committee staff first met with Comcast, its data retention period for a customer's IP address assignments was 30 days. Just prior to the June hearing, Comcast announced that it was increasing this data retention period to six months beginning in September 2006. AOL, Yahoo!, Microsoft, and Earthlink announced that they were joining together to create the Technology Coalition at NCMEC, the purpose of which is to establish a central clearinghouse of known images of child pornography and to develop technology solutions to combat online child pornography. Also, in response to staff concerns, Google strengthened its advertising policies to ensure that it was not accepting advertising from companies with links to websites that promote the sexual exploitation of children. Finally, as mentioned previously, MySpace recently announced that it will build a sex offender database in order to screen its site for users who are also registered sex offenders.

Following the June hearings, Committee staff traveled to the Netherlands and Belgium in order to meet with Dutch and European Union officials to discuss their progress in implementing a European Union data retention directive. The directive, which was issued on March 15, 2006, is broader than the policies discussed by the Internet Service Providers who testified at the Subcommittee's June hearing because it applies not only to data that links an IP address to a particular individual, but to network and cellular telephones including the records of telephone numbers called and the date and time of Internet access. Pursuant to the directive, European Union member countries must adopt a data retention policy of at least six months and no more than two years for the data covered by the directive. Committee staff discussed with European Union and Dutch officials the response of the European Member countries to the directive; the reaction of the Internet Service Provider industry; technical issues posed by the directive; and cost projections for implementing the initiative. According to the directive, Member

countries must have approved implementing legislation for Internet Service Providers data retention by March 15, 2009. Therefore, any U.S. ISP that is also doing business in an E.U. member country will need to comply with this legislation. Notably, no ISPs were able to provide the E.U. with substantive cost estimates for implementing the data retention legislation.[22]

C. The Role of the Financial Services Industry in Combating the Sexual Exploitation of Children Over the Internet

On September 21, 2006, the Subcommittee held a hearing entitled "Deleting Commercial Child Pornography Sites from the Internet: The U.S. Financial Industry's Efforts to Combat this Problem" that focused on the efforts of the financial industry to prevent commercial child pornography businesses and purchasers of child pornography from using their payment systems. The purpose of the hearing was two-fold. First, the Subcommittee hoped to learn how credit card companies and the banks that are members of their systems, known as merchant or acquiring banks, attempt to prevent commercial child pornography businesses from using their payment networks to facilitate the sale and distribution of child pornography images. In addition, the Subcommittee was interested in the efforts of the National Center on Missing and Exploited Children to create the Financial Coalition Against Child Pornography at NCMEC, or "Financial Coalition," and how it intended to achieve its stated goal of eradicating commercial child pornography over the Internet by 2008.

The first panel of witnesses focused on how law enforcement agents investigate online commercial child pornography businesses and the difficulties presented in these investigations. The witnesses on this panel included Mr. Christopher Christie, United States Attorney for the District of New Jersey, Mr. James Plitt, Director of the Cyber Crimes Center at U.S. Immigration and Customs Enforcement ("ICE"), U.S. Department of Homeland Security, and Mr. Ernie Allen, President and C.E.O. of NCMEC. Both Mr. Christie's and Mr. Plitt's testimony focused on the RegPay investigation. RegPay, also known as Operation Falcon, was the first international commercial child pornography website ring to be investigated and prosecuted in the United States. Mr. Christie, whose office extradited and prosecuted the defendants in the U.S., and Mr. Plitt, whose department was the lead law enforcement agency, explained how a company in the former Soviet republic of Belarus, called "RegPay," operated several commercial child pornography websites as well as processed payments for over 50 other child pornography websites. The Belarus firm used a U.S.–based credit card processing company, called Connections USA, to process the monthly payments for access to the websites containing images of child pornography. United States Attorney Christie described how his office worked cooperatively with federal, local and international law enforcement to prosecute the persons in Belarus operating the websites. Ultimately, the investigation led to the arrest of over 300 persons in the United States that purchased child pornography from this website and over 1,400 arrests worldwide. The two defendants from Belarus involved

[22] Member countries are handling the legislation in different ways; the U.K. has opted to pay for the cost of retention and storage up to an agreed upon amount.

in the RegPay case were extradited to the United States, pled guilty on the eve of trial and were sentenced in August 2006 to 25 years in prison and a fine of $25,000 each. Also, $1.15 million was seized as part of their illegal business operations that sexually exploited children.

In addition to using the RegPay case as a model for future investigations, United States Attorney Christie, Mr. Plitt, and Mr. Allen noted that the payment methods used by commercial child pornography businesses are evolving. Specifically, law enforcement agents have witnessed the rapid growth of anonymous forms of payment to purchase child pornography images over the Internet. These forms of payment include digital currencies. Typically, digital currency is created when an Internet user makes a deposit to an account either from a bank account using an electronic funds transfer or by credit card. The digital currency account is then used to make purchases on the Internet. According to Mr. Plitt, digital currencies often make it difficult for law enforcement agents to identify and track the global financial structure that facilitates Internet child exploitation. As Committee staff has learned during the course of its investigation, this is because some digital currency companies do not request information relating to the identity of the account holder or they do not attempt verify it.

In his testimony, Mr. Allen also addressed the work of NCMEC's Financial Coalition. The primary purpose of the Financial Coalition, as Mr. Allen described it, is to "follow the money, stop the payments, shut down the account, and put an end to this multi-billion dollar enterprise." The principal obstacle to shutting down the websites that sell sexually exploitative images of children is identifying the merchant that is processing payments for those images. In order to shut down the merchant's website and prevent it from processing payments, law enforcement agents must first identify the merchant bank or acquiring bank that actually approved a merchant for participation in the credit card networks. Usually, the credit card companies, like VISA, MasterCard, and American Express, do not have control over the website or a direct relationship with the merchant that is selling the illegal material. Therefore, it is impossible for the credit card companies themselves to immediately terminate the child pornography websites that are purportedly accepting their credit cards for payment. The role of the Financial Coalition is to assist in quickly identifying the merchant or acquiring banks that process payments for the commercial child pornography businesses, and facilitate the transmission of that information to law enforcement. To do so, NCMEC and the Financial Coalition launched a pilot "Clearinghouse" in the summer of 2006 to facilitate better and faster communication between the financial industry and law enforcement, when a commercial child pornography site is identified. The methods which the Financial Coalition are using to detect and track down the merchant associated with the particular commercial child pornography site, however, are confidential and cannot be discussed in detail in this report. As of the hearing, Mr. Allen stated that 87 percent of the United States payments industry, as measured in dollars running through the payments system, has joined the Financial Coalition.

Mr. Allen also described another new initiative being undertaken by NCMEC to combat online child pornography. According to Mr. Allen, based on the Committee's

suggestion, NCMEC is working with several U.S.–based Internet Service Providers to develop a proactive program for terminating websites that contain images of child pornography. Under this program, a NCMEC analyst will first identify the websites that contain images of child pornography. The addresses of those websites will then be forwarded to federal and state law enforcement agents so that they can initiate an investigation, if appropriate. After law enforcement is notified, NCMEC will then forward the websites' addresses to the Internet Service Providers who are registered with and reporting to NCMEC and request that they enforce their terms of service, which prohibit illegal content. These ISPs have agreed to terminate the website upon such notice and use filters to block access through their systems to those websites. This is an important step toward implementing a system that will block Internet subscribers' attempts to access websites containing child pornography images. We remain concerned, however, that, this initiative may not have the support of all U.S. ISPs. While many major ISPs in the United States are interested in the initiative, hundreds of others are not even registered with or reporting into the Cybertipline and their support for this initiative is unclear.

The second panel was comprised of witnesses from the credit card associations, including American Express, MasterCard, and VISA, and other payment companies, including e-Gold and PayPal. The purpose of this panel was to examine the payments industry's efforts to prevent individuals from using their systems to process child pornography transactions. Although MasterCard and VISA do not sign up merchants or card holders directly — this is the responsibility of their member banks, known as merchant banks — they do set the policies and conditions their merchant banks must follow for approving a merchant.[23] In addition to determining the categories of business in which their merchants may engage, MasterCard and VISA dictate the procedures and guidelines the merchant banks must follow with regard to screening prospective merchant accounts both before and after they begin processing payments as well as closely monitor the merchant banks' credit policies. As MasterCard, VISA and American Express explained in their testimony, their standards for approving Internet merchants are stricter than for "brick and mortar" merchants because Internet merchants inherently present a greater risk.

In addition to adopting standards intended to identify potential or approved merchants who engage in illegal activity, such as commercial child pornography, American Express, VISA, and MasterCard also have implemented, with varying degrees of success, proactive measures to ensure that their Internet merchants are not selling or dealing in child pornography. The principal proactive measures adopted by these companies is "spidering," or crawling the web, in order to identify websites that claim to

[23] American Express operates differently from MasterCard and VISA in that American Express itself both issues credit cards to its credit card holders and acquires, or approves, the merchants who can accept American Express. In addition, the companies' policies differ with regard to the categories of business they will accept. American Express has a blanket prohibition against signing up merchants involved in the adult pornography industry. Companies such as MasterCard and Visa have terms within the bylaws of their association agreements that may prohibit certain adult content. Some acquiring banks may have an expanded definition of prohibited businesses that goes beyond what the credit card association rules prohibit.

accept American Express, MasterCard, or Visa and are participating in illegal activity or are violating the intellectual property rights of the companies by purporting to accept credit cards in an effort to make the website look legitimate. Once the credit card association determines that the website accepts their credit cards and is engaged in child pornography, the credit card association may shut down the merchant's account or fine the merchant. In addition, the credit card companies report the website to NCMEC or, in some cases, directly to law enforcement, or both.

Interestingly, the credit card associations explained in their testimony and in meetings with Committee staff that they have discovered relatively few instances where merchants were participating in a commercial child pornography business. They maintain that the majority of child pornography websites that claim to accept major credit cards, such as American Express, MasterCard, or Visa, in fact do not. Instead, when a child pornography purchaser clicks on the payment link, the website will lead the purchaser to other payment methods. According to the credit card associations, their strict policies and procedures for approving merchants are successful in screening out merchants who intend to engage in this illegal activity.

Like the credit card associations, PayPal and e-Gold, which are alternative payment mechanisms or digital currencies, have also adopted policies and procedures that prohibit their users from using their account to purchase child pornography. PayPal, a subsidiary of eBay, has taken steps to identify and minimize the use of its services for illegal transactions. For example, PayPal's policies state that its users may not use their accounts to purchase "any obscene or sexually oriented goods or services." While their policies prohibit the purchase of child pornography, the critical issue with digital currencies with respect to commercial child pornography is the anonymity it offers its users. PayPal testified, however, that its system provides accountability and traceability because each individual user is required to provide his or her name, full address as it appears on the financial instrument funding the account, and home telephone number. Similarly, business users are required to provide information about their business, the name of the business owner, and work telephone and address information. PayPal then verifies this information against external and internal databases. Also, PayPal, like the credit card associations, performs some due diligence on its merchants as well as ongoing fraud and credit review after the merchant is approved to accept PayPal.

While e-Gold is also a digital currency, it operates differently from PayPal in that its accounts are purportedly backed by actual gold reserves. To establish an account, an individual completes a short form online, including some identifying information. However, e-Gold does not verify this identification information or require that a credit card or other financial instrument be presented to verify identity. Further, e-Gold does not maintain sufficient records reflecting the activity of e-Gold accounts or, unlike credit card associations and merchant banks, conduct any due diligence on the merchants that accept e-gold.

The Subcommittee's investigation into the use of financial instruments to purchase child pornography over the Internet revealed a much larger problem touching

upon the burgeoning industry of digital currencies: the lack of regulation of digital currencies by any government entity, domestic or foreign. Digital currencies that do business in the U.S. are not subject to any of the U.S. banking requirements. This has created a dangerous loophole in commercial transactions occurring on the Internet with virtually no accountability. It is imperative that the U.S. and other countries address the rise of digital currency and begin to subject this industry to some form of oversight and regulatory consistency. As of now, operations such as e-Gold are available to individuals who wish to transfer money anonymously for any purpose, whether legal or illegal.

The third panel focused on the efforts of acquiring banks or merchant processing companies to prevent commercial child pornography merchants from having access to a traditional method of online payment, such as a credit card, to offer on their site. The witnesses included Chase Paymentech and Bank of America, which are both acquiring banks, and NOVA and First Data, which are merchant processors.[24] As the witnesses explained at the hearing, before an acquiring bank or merchant processor can conduct merchant processing, that merchant must first be approved by the bank. The acquiring bank or processing company will first determine whether the merchant's business is consistent with its credit policies, as well as the association's policies. Bank of America, First Data Corporation, and NOVA each testified that their credit policies forbid them from approving any merchant who engages in certain types of businesses, including any illegal activity, such as child pornography, as well as certain legal activity, such as adult pornography.

After the merchant bank concludes that the merchant's business is consistent with its credit policies and the credit card association's policies, the merchant bank will then conduct an underwriting and risk review. Most institutions conduct a more rigorous review of Internet merchants, as opposed to brick and mortar merchants, because Internet merchants are a greater credit risk. For example, Bank of America and Chase review each page of a prospective Internet merchant's website to determine that the links on the site are operational, that they do not link to illegal or prohibited content, and that the merchant has appropriate customer service and product information. Once a merchant has been approved, the acquiring banks or processors then conduct varying levels of ongoing review to ensure that the merchant does not begin to offer banned products or services, such as adult content or child pornography. According to the witnesses, this review is primarily automated and involves monitoring trends in sales volume and average sales ticket size in order to identify patterns that may indicate illegal activity. If unusual activity is noted, the acquirer will conduct a more extensive review of the merchant's business. In addition, some acquirers, like Bank of America, attempt to visit the websites of Internet merchants at least one time a year, even if abnormal activity is not present; other acquirers, such as First Data, will revisit a merchant's website only if certain risk factors are triggered during its ongoing review. Finally, MasterCard and American Express acquiring banks are required to check the prospective merchant

[24] First Data and NOVA are not banks; various acquiring banks may contract out certain of their merchant banking functions, such as performing due diligence on prospective merchants and other functions, to these companies. Therefore, given the large size of their portfolio of merchant banks, much of the due diligence on the merchant side is frequently done by merchant processing companies like First Data or NOVA

information against a database known as the MATCH system, which houses information about terminated merchants.

In addition to ongoing monitoring of merchants, the merchant banks or processors also take additional proactive steps to identify merchants engaged in commercial child pornography. NOVA Information Systems uses a web crawler to search for certain search terms that may suggest a site contains child pornography. However, not all merchant banks or processors do so, contending it is unnecessary because the card associations already use web crawling services and inform their merchant banks when the crawlers find child pornography. Like the credit card associations, the merchant and acquiring banks identified only a handful of merchants engaged in commercial child pornography in a given year. Typically, according to the banks, when the merchant applied for an account, its business and its website appeared to be legitimate; however, sometime after obtaining an account, the merchant then began to engage in commercial child pornography. The witnesses believe that the number of child pornography businesses they identify is minimal because their credit policies prohibit all pornography, even adult pornography, and their credit and underwriting review is successful in identifying risk factors that are linked to illegal activity.

There is an obvious discrepancy between the number of websites that engage in commercial child pornography — approximately 100,000 or more as estimated by the FBI — and the number of child pornography merchants identified by mainstream credit card companies. This discrepancy may be attributable to several factors, including the popularity of alternative payment methods, such as digital currencies; the use of barter, such as providing new images of child pornography to "pay" for child pornography received from a website; and the fact that commercial child pornography websites are skilled at masking the true nature of their business.

D. **The Psychology of Pedophiles and Child Predators**

On September 26, 2006, the Subcommittee convened a hearing dedicated to exploring the psychology of pedophiles and child predators as well as how the commercial child pornography industry is evolving over the Internet.

The first panel of witnesses addressed the psychology and behavior of child predators. The witnesses included Dr. Anna C. Salter, a clinical psychologist in Madison, Wisconsin who treats and studies sex offenders; Dr. Andres C. Hernandez, Director of the Bureau of Prisons' Sex Offender Treatment Program at the Federal Correction Institution at Butner, NC; and Dr. Philip Jenkins, a Professor of Religious Studies and History at Pennsylvania State University who wrote a book in 2001 entitled Beyond Tolerance: Child Pornography on the Internet which described what he observed after joining pedophile forums on the Internet and observing pedophiles' conversations.

The New York Times reporter Kurt Eichenwald also joined the panel to discuss his two recent articles published on August 20 and August 21, 2006, entitled "With Child

Sex Sites on the Run, Nearly Nude Photos Hit the Web" and "From Their Own Online World, Pedophiles Extend Their Reach," respectively. The first article discussed websites commonly referred to as "child modeling websites," where young girls are posed provocatively in sexual clothing. According to Mr. Eichenwald's investigation, the owners and operators of these websites have deliberately posed the girls in clothing because they believe that the current definition of "child pornography" requires the genitalia to be somehow visible in order for the images to be illegal. The second article focused on the online forums and chatrooms visited by pedophiles and child predators, where Mr. Eichenwald observed child predators encouraging one another and rationalizing their behavior.

Dr. Hernandez's testimony focused on the treatment of sex offenders within the Bureau of Prisons ("BOP"). Dr. Hernandez runs the BOP's only Sex Offender Treatment Program. Currently, that treatment program can only house 112 inmates at a time, out of the almost 12,000 federal prisoners now incarcerated for sexual crimes. The program is wholly voluntary for offenders. The treatment program lasts 18 months and is conducted in seven phases; these phases include a complete psychiatric evaluation and group and individual therapy. The final phase includes a polygraph. During the polygraph, inmates are questioned about whether they have committed contact offenses for which they have not been arrested or convicted. The information provided during the polygraph was the basis for a presentation Dr. Hernandez gave in 2000 entitled "Self-Reported Contacted Sexual Offenses by Participants in the Federal Bureau of Prisons' Sex Offender Treatment Program: Implications for Internet Sex Offenders." With regard to the inmates he had treated, Dr. Hernandez found that 76 percent of the inmates convicted on charges related to the possession of child pornography or luring a child had also committed sexual contact offenses against children. Dr. Hernandez believed that this finding suggested that the majority of sex offenders convicted of Internet sex crimes had "similar behavioral characteristics as many child molesters."

In her testimony, Dr. Salter confirmed that a "considerable percentage" of individuals convicted for child pornography crimes had also committed contact offenses. More disturbingly, in her testimony, Dr. Salter's suggested that this number may be underestimated, as one report found that only three percent of individuals who have committed contact offenses are caught. In addition to finding a link between possessing child pornography and committing contact offenses, Dr. Salter also testified that she believes there is a link between viewing online pornography and committing contact offenses. With regard to reducing the number of contact offenses against children, both Dr. Jenkins and Dr. Salter testified that reducing online child pornography would also reduce contact crimes, especially among those offenders who are emboldened to act on their sexual desires or urges by viewing child pornography. According to Dr. Salter, "child pornography increases the arousal to kids and is throwing gasoline on the fire."

As Dr. Salter acknowledged, while recidivism is common among sex offenders, treatment can be successful in reducing it. One report cited by Dr. Salter found that recidivism among sex offenders can be reduced by as much as 40 percent with proper treatment. Dr. Salter and Dr. Hernandez agreed that cognitive behavioral therapy or

treatment was most effective in treating sex offenders; however, Dr. Salter testified that many states do not have the resources to provide the treatment that might decrease recidivism and, in fact, that some states have waiting lists for treatment.

Mr. Eichenwald's testimony focused on the online pedophile community. Mr. Eichenwald described the online pedophile community as being very sophisticated and cunning. For example, Mr. Eichenwald testified that there are Internet podcasts and even an Internet radio station organized by pedophiles for adults who are attracted to children. During the four months Mr. Eichenwald spent examining pedophile forums and chatrooms, he observed pedophiles discussing the best ways to get access to children, including serving as camp counselors, foster care parents, and other community events where children gather, and rationalizing their behavior. For example, some of the pedophiles Mr. Eichenwald observed believe their relationships with minors are consensual and that the child, in fact, instigated the relationship. In fact, Mr. Eichenwald found that some pedophiles see themselves as leaders of a "cause" to advance the rights of *children* to have sex with adults. The pedophiles Mr. Eichenwald observed also rationalized their behavior in other ways, arguing that adults who attempt to protect children from them are "child haters" and impeding children's happiness.

Perhaps even more disturbing is the physical proximity to children the pedophiles observed by Mr. Eichenwald online seemed to enjoy. Mr. Eichenwald testified that the pedophile conversations he observed included daily accounts of their observations of children. Many of the people who visited the forums were teachers and school administrators, pediatricians, and other individuals with access to children.

The second panel of witnesses focused on the role of web hosting companies. The witnesses included Mr. Thomas Krwawecz, the C.E.O. and President of Blue Gravity Communications, Inc., and Ms. Christine Jones of GoDaddy.com. Blue Gravity is a relatively small web hosting business located in Pennsauken, N.J., with servers located in Philadelphia, PA; GoDaddy.com is the number one registrar of domain names in the world and is also a large and web hosting company. Web hosting companies provide the connection to the Internet for website operators and own the servers where websites upload their content. Mr. Krwawecz and Ms. Jones discussed how their companies identify possible child pornography or child modeling websites either when those websites register their domain names or during the hosting process.

As Ms. Jones described, the first step in creating the website is registering, and therefore reserving, the domain name. At GoDaddy.com, the domain registration process is entirely automated. Ms. Jones testified that it would be very difficult to prevent an online child pornography or child modeling website from registering for a domain name because it is difficult, if not impossible, to verify the legitimate use of the domain name even if the name suggests it may be a child pornography website.

According to the witnesses, once a website name is registered and a web hosting company begins hosting content, it is still difficult for the web hosting company to search proactively the websites it hosts in order to uncover child pornography content. Mr.

Krwawecz testified that, in his experience, employing a web crawler service that uses certain terms found on child pornography websites would be impractical because the search would turn up thousands of results, most of which do not contain child pornography content. As mentioned previously, financial services companies do employ web crawlers as well as conduct other searches in order to identify inappropriate content.

Ms. Jones and Mr. Krwawecz also explained that they typically learn that websites they host contain inappropriate content through reports or complaints from outside parties. Once a report is made, Ms. Jones testified that GoDaddy.com initiates an investigation to determine if the website contains child pornography or child modeling and immediately suspends and reports websites that contain child pornography content. With regard to child modeling websites, Ms. Jones stated that GoDaddy.com routinely suspends websites that show images of children posed in a manner intended to be "explicitly sexy"; posed in adult lingerie; or children who are partially nude or in very little clothing "not associated with normally acceptable situations." Similarly, Mr. Krwawecz stated that it is the policy of his company to investigate the reports it receives and to disable the accounts of websites that contain "blatant illegal content." However, with regard to potential child modeling websites, Mr. Krwawecz states that his company requests proof of age for the models from the website, and if "satisfactory proof" cannot be provided, the website is terminated. Although websites hosted by Mr. Krwawecz's company included sexually solicitous posing of children who appeared as young as eight or nine-years-old, there is no evidence that Mr. Krwawecz was aware of this content and, once notified of the websites prior to the hearing, immediately terminated them.

As noted earlier, web hosting companies, domain registries, credit card companies, social networking sites, and cellular telephone carriers, are not clearly subject to the reporting requirements of 42 U.S.C. § 13032 or other provisions. While certain financial services companies have taken a proactive approach to working with NCMEC on the problem of commercial child pornography websites, and in reporting into the CyberTipline without a legal obligation to do so, not all firms that profit from these websites have followed suit. More importantly, many industries do not even know about the CyberTipline or whether they can, should, or must report into the CyberTipline. For example, due to the urging of NCMEC and a question posed by the Subcommittee at the June 28th hearing, in August 2006, the FCC issued an advisory opinion that cellular telephone carriers would not be precluded by other statutory requirements from complying with the reporting requirements of 42 U.S.C. § 13032.

Without any mechanism by which to track the number of Internet Service Providers, web hosting companies or domain registries in the U.S., it is also difficult to give notice to these entities of their statutory obligations, the existence of the CyberTipline, NCMEC, and the VGT, as well as the development of best practices. Clearly, neither current legal requirements nor voluntary action have been apparently sufficient to put a significant dent in the problem of sexual exploitation of children over the Internet.